UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/676,748	09/29/2000	Andrew Edward Nunns	9219-4	2283

				EXAMINER
20792	7590	06/23/2004		NOBAHAR, ABDULHAKIM

MYERS BIGEL SIBLEY & SAJOVEC
PO BOX 37428
RALEIGH, NC 27627

ART UNIT	PAPER NUMBER
2132	3

DATE MAILED: 06/23/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

PTO-90C (Rev. 10/03)

	Application No.		Applicant(s)	
Office Action Summary	09/676,748		NUNNS, ANDREW EDWARD	
	Examiner		Art Unit	
	Abdulhakim Nobahar		2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE <u>3</u> MONTH(S) FROM
THE MAILING DATE OF THIS COMMUNICATION.
- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed
  after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
  Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any
  earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☐ Responsive to communication(s) filed on _____.

2a)☐ This action is **FINAL**.   2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is
closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-50* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-4,11,14-18,21-23,25-28,32,33,36-42,44-47,49 and 50* is/are rejected.

7)☒ Claim(s) *5-10,12,13,19,20,24,29-31,34,35,43 and 48* is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All   b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage
application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1)☒ Notice of References Cited (PTO-892)

.2)☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3)☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date <u>2</u>.

4)☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5)☐ Notice of Informal Patent Application (PTO-152)

6)☐ Other: _____.

DETAILED ACTION

Claim Rejections - 35 USC § 112

The following is a quotation of the first paragraph of 35 U.S.C. 112:

> The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

Claims 1, 14-16, 17, 19, 20- 22, 24-26, 27, 29-32, 37, 43, 45-47 and 50 are rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the written description requirement. The claim(s) contains subject matter, which was not described in the specification in such a way as to reasonably convey to one skilled in the relevant art that the inventor(s), at the time the application was filed, had possession of the claimed invention.

Claims 1, 16, 17, 20-22, 26, 27, 32 and 37 recite "at least ... during a first time interval". The "first time interval" has not been described in the specification and has not been disclosed in the specification that where this time interval is located during the period of operation of a programmable logic device. Appropriate correction is required.

Claims 14, 15, 17, 19, 20, 22, 24, 25, 29, 30, 31, 45, 46, 47 and 50 recite "weakly random sequence of bits". The specification does not describe that what kind of stream bits is a weakly random sequence of bits. Appropriate correction is required.

Claims 19, 24 and 43 contain "dead man switch", which has not been described

in the specification. Appropriate correction is required.

Claim 20 on lines 2 and 3 recites "a respective point in the first time interval",

which has not been described in the specification. Appropriate correction is required.

The following is a quotation of the second paragraph of 35 U.S.C. 112:

The specification shall conclude with one or more claims particularly pointing out and distinctly
claiming the subject matter which the applicant regards as his invention.

Claim 38 recites the limitation "ASICs and PLDs" in lines 2 and 3. There is

insufficient antecedent basis for these limitations in the claim. Appropriate correction is

required.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that

form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(b) the invention was patented or described in a printed publication in this or a foreign country or in public
use or on sale in this country, more than one year prior to the date of application for patent in the United
States.

Claims 1, 3, 16, 18, 21, 23, 26, 32, 37-39 and 44 are rejected under 35

U.S.C. 102(b) as being anticipated by Priem et al. (5,652,793; hereinafter Priem).

Claim 1

Priem discloses a method and apparatus for controlling the operation of a

computer system (corresponding to the recited programmable logic device) (col. 2, line

59-col. 3, line 10). Priem also discloses an encoding circuit (corresponding to the recited

integrated circuit) that generates a verification value (corresponding to the recited a

second encrypted data stream) by using a secret key to encode a concatenated value.

The concatenated value is produced from concatenating an application identifier

(corresponding to the recited a first data stream) and a secret plaintext value (col. 4,

lines 38-44). Priem further discloses that the verification value is sent to a comparison

circuit (corresponding to the recited authorization device) to be compared with a

password whether to allow the software to be run on the computer system (col. 4, lines

44-52). This comparison is performed (col. 2, lines 5-10 and col. 4, lines 27-37) at

intervals (corresponding to the recited periodically) each time the application program is

run (examiner interprets that "during first time interval" means the beginning of running a

program).

Claim 3

Priem discloses:

Wherein said integrated circuit component utilizes an encryption operation to generate the second encrypted data stream from the first data stream (col. 3, lines 54-56; col. 5, lines 25-32).

Claims 16, 21, 26 and 44

Priem discloses:

An integrated system (see Fig. 1), comprising:

an authorization device that generates a first encrypted data stream (col. 4, lines 3-17, where the password which is an encrypted data stream corresponds to the recited first encrypted data stream);

a programmable logic device that generates a second encrypted data stream while simultaneously operating under at least partial control of configuration data during a first time interval (col. 4, lines 37-44, where the verification value corresponds to the recited second encrypted data stream generated by the an encoding circuit of a computer system corresponding to the recited a programmable logic device and it is interpreted by the examiner that the "during a first time interval" means the beginning of program operation); and

authorization detection circuitry that at least periodically compares the first and second encrypted data streams during the first time interval and disables operation of said programmable logic device if the first and second encrypted data streams indicate that said programmable logic device is not authorized to utilize the configuration data

(col. 4, lines 44-52; Fig. 2, where the comparison circuit corresponds to the recited

authorization detection circuitry).

Claims 18 and 23

Priem discloses:

The system of Claim 16, wherein said authorization detection circuitry is internal

to said programmable logic device (col. 4, lines 44-48, where the comparison circuit 30

corresponds to the recited authorization detection circuitry which is part of the computer

system 10 corresponding to the recited programmable logic circuit); wherein said

programmable logic device utilizes an encryption operation to generate the second

encrypted data stream (see Fig. 2, col. 3, lines 54-56, col. 4, lines 40-44 and col. 5,

lines 24-27, where the verification value which is an encrypted data stream is produced

by an encryption operation utilized by the circuitry of the computer system

corresponding to the recited programmable logic device); and wherein each of a

plurality of bits in the second encrypted data stream is determined by evaluating at least

one bit in the first encrypted data stream (see Fig. 2, where comparator 30 compares

the bit stream of the verification value with the bit stream of the password which is an

encrypted data stream).

Claims 32 and 37

Priem discloses:

An authorization device, comprising:

a first integrated circuit component (col. 4, lines 35-37, where the encoding circuit

corresponds to the recited first integrated circuit) that in response to a first data stream

generated external to said first component (col. 4, lines 33-35, where the application

identifier corresponding to the recited a first data stream generated outside the

encoding circuit col. 4, lines 3-10) generates a second data stream (col. 4, lines 40-45,

the verification value) that is at least periodically evaluated by a distinct second

integrated circuit component (col. 4, lines 44-47, where the comparison circuit

corresponds to the recited second integrated circuit and the comparison operation is

performed at intervals during each time the program is run) to assess whether

performance of operations within the second integrated circuit component are

authorized during a time interval when the first data stream is being generated (col. 4,

lines 46-52, examiner interprets that the recited the second integrated circuit refers to

the programmable logic device and the first data stream refers to the data stream being

generated in response to received or inputted first data stream).

Claim 38

Priem discloses:

The system of Claim 37, wherein said second component comprises an

integrated circuit selected from the group consisting of ASICs and PLDs (col. 2, lines 1-

5; col. 2, line 60-col. 3, 10).

Claim 39

The system of Claim 37, wherein said second component generates the first data stream (col. 4, lines 37-50, where the encoding circuit generates the encrypted verification value); and wherein said first and second components comprise first and second stream encryptors therein, respectively (col. 4, lines 5-10 and col. 4, lines 40-44).

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 2, 11, 33, 40 and 41 are rejected under 35 U.S.C. 103(a) as being unpatentable over Priem et al. (5,652,793; hereinafter Priem) in view of Lacey (6,651,181 B1).

Claims 2, 33, 40 and 41

Priem discloses a method for authorizing operation of an application program on a computer (corresponding to the programmable logic device) (see abstract). Priem also discloses that different the computer components (i.e., integrated system) are

connected to each other by a single bus (see Fig. 1). Priem, however, does not

expressly disclose that the data streams are being time division multiplexed during the

process of authorization of the program operation.

Lacey disclose a clocking scheme for programmable logic device comprising

circuits that, for example, generates a second plurality of clock signals (corresponding

to the recited data stream) in response to a first plurality of clock signals (col. 2, lines

10-20). Lacey further discloses the use of a multiplexer that produces signals from one

or more input signals by utilizing time division multiplexing technique (col. 3, lines 15-

55).

It would have been obvious to a person of ordinary skill in the art at the time the

invention was made to implement a time division multiplexing circuit as taught in Lacey

in the method and apparatus of Priem, because it would yield a higher performance with

fewer device resources (col. 2, lines 1-7).

Claim 11

Priem discloses:

Wherein said integrated circuit component utilizes an encryption operation to

generate the second encrypted data stream from the first data stream (col. 3, lines 54-

56; col. 5, lines 25-32).

Claim 4, 5, 12, 14, 15, 17, 22, 25, 27, 28, 36, 42, 45-47, 49 and 50 are rejected

under 35 U.S.C. 103(a) as being unpatentable over Priem et al. (5,652,793; hereinafter

Priem) in view of Folmsbee (6,609,201 B1).

Claims 4, 5, 12 and 42

Priem discloses a method for authorizing operation of an application program on

a computer (corresponding to the programmable logic device) (see abstract). Priem,

however, does not expressly disclose a circuit to intentionally insert error into the

second encrypted data stream.

Folmsbee teaches a CPU (microprocessor) for secure execution of programs

that includes a reconfigurable logic circuitry for processing instructions from an

instruction buffer included in the microprocessor (col. 2, lines 15-33). Folmsbee further

teaches a circuitry for generating errors and intentionally inserting into the data

encrypted stream (col. 8, line 66-col. 9, line 15; Fig. 3). Folmsbee also teaches a

permutation function for producing a data bit stream that is a combination of encrypted

codes and other codes such as error correction codes (col. 8, lines 32-44)

It would have been obvious to a person of ordinary skill in the art at the time the

invention was made to implement a permutation function and a circuitry to intentionally

insert errors into the encrypted data stream as taught in Folmsbee in the method and

apparatus of Priem, because it would provide an encryption scheme which prevents

unauthorized persons from "attacking" the encryption of the software through analysis

of the input and output of user commands and instruction sets from the software (col.

2, lines 2-15).

Claims 14, 15, 17, 22, 27 and 45

Priem discloses a method for authorizing operation of an application program on

a computer (corresponding to the programmable logic device) (see abstract). Priem also

discloses that a verification value (corresponding to the recited first encrypted data

stream) is generated based on a concatenated plaintext value and an application

identifier (corresponding to the recited a first data stream) (col. 4, lines 37-44). Priem,

however, does not expressly disclose the use of a random number generator to

generate random sequence of bits to be used for generation of encrypted data stream.

Folmsbee discloses a random number generator that is configured to produce

random sequence of bit stream (col. 9, lines 27-36; col. 11, lines 24-30).

It would have been obvious to a person of ordinary skill in the art at the time the

invention was made to implement a random number generator coupled to the

integrated circuit to generate random sequence of data stream as taught in Folmsbee

in the method and apparatus of Priem, because it would provide an encryption scheme

which prevents unauthorized persons from "attacking" the encryption of the software

through analysis of the input and output of user commands and instruction sets from

the software (col. 2, lines 2-15).

Claims 25 and 46

Priem discloses a method for authorizing operation of an application program on a computer (corresponding to the programmable logic device) (see abstract). Priem also discloses that the authenticator including a comparison circuit (corresponding to the recited authorization device) is coupled to the control processor (corresponding to the recited integrated circuit) by a bus (see Fig. 1). Priem, however, does not expressly disclose that the data streams are being time division multiplexed during the process of authorization of the program operation.

Folmsbee teaches a CPU (i.e., microprocessor) for secure execution of programs that includes a reconfigurable logic circuitry for processing instructions from an instruction buffer included in the microprocessor (col. 2, lines 15-33). Folmsbee further teaches the use of a multiplexer as a part of the control logic system for multiplexing two streams of data (col. 6, lines 10-35).

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to implement a multiplexer as a part of the programmable logic device (i.e., coupled to the integrated circuit) for time division multiplexing two data streams as taught in Folmsbee in the integrated circuit of Priem computer system, because it would facilitate the control of other functions such as an error correction operation (col. 6, lines 24-31).

Claim 28

Priem discloses:

The method of Claim 27, wherein the first encrypted data stream is generated internal to the programmable logic device (see col. 4, lines 37-44, where the verification value is produced inside the computer) and the second encrypted data stream is generated external to the programmable logic device (see col. 4, lines 20-25, where the password, the second encrypted data stream is generated outside the computer).

Claims 47 and 50

Priem discloses a method for authorizing operation of an application program on a computer (corresponding to the programmable logic device) (see abstract). Priem also discloses that an encoding circuit (corresponding to the recited a first integrated circuit) generates a verification value (corresponding to the recited first encrypted data stream) (col. 4, lines 37-44). The verification value is produced by encoding (i.e., encrypting) a value obtained from the concatenation of a plaintext value and an application identifier (corresponding to the recited a first data stream) (col. 4, lines 37-44). Priem further discloses that an encrypted value named password (corresponding to the recited the second data stream) is generated in a separate integrated circuit (corresponding to the recited second integrated circuit) (col. 4, lines 7-15). Priem, however, does not expressly disclose the use of a random number generator to generate random sequence of bits to be used for generation of encrypted data stream.

Folmsbee discloses a random number generator that is configured to produce random sequence of bit stream (col. 9, lines 27-36; col. 11, lines 24-30).

It would have been obvious to a person of ordinary skill in the art at the time the
invention was made to implement a random number generator coupled to the
integrated circuit to generate random sequence of data stream as taught in Folmsbee
in the method and apparatus of Priem, because it would provide an encryption scheme
which prevents unauthorized persons from "attacking" the encryption of the software
through analysis of the input and output of user commands and instruction sets from
the software (col. 2, lines 2-15).

Allowable Subject Matter

Claims 6-10, 13, 19, 20, 24, 29-31, 34, 35, 36, 43, 48 and 49 are objected to as
being dependent upon a rejected base claim, but would be allowable if rewritten in
independent form including all of the limitations of the base claim and any intervening
claims.

Conclusion

The prior art made of record and not relied upon is considered pertinent to
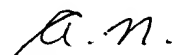applicant's disclosure.

US Patent No. 5,724,425 to Chang et al

US Patent No. 5,892,683 to Sung

US Patent No. 4,888,798 to Earnest

Any inquiry concerning this communication or earlier communications from the

examiner should be directed to Abdulhakim Nobahar whose telephone number is 703-

305-8074. The examiner can normally be reached on M-F 8-5.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's

supervisor, Gilberto Barron can be reached on 703-305-1830. The fax phone number

for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the

Patent Application Information Retrieval (PAIR) system. Status information for

published applications may be obtained from either Private PAIR or Public PAIR.

Status information for unpublished applications is available through Private PAIR only.

For more information about the PAIR system, see http://pair-direct.uspto.gov. Should

you have questions on access to the Private PAIR system, contact the Electronic

Business Center (EBC) at 866-217-9197 (toll-free).

Abdulhakim Nobahar
Examiner
Art Unit 2132

AN
June 3, 2004

GILBERTO BARRON
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100